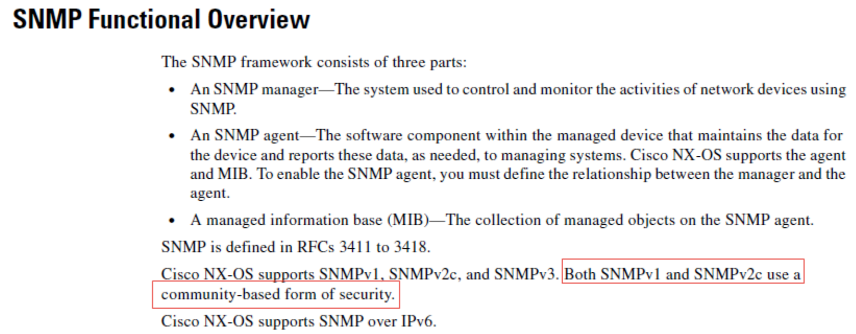
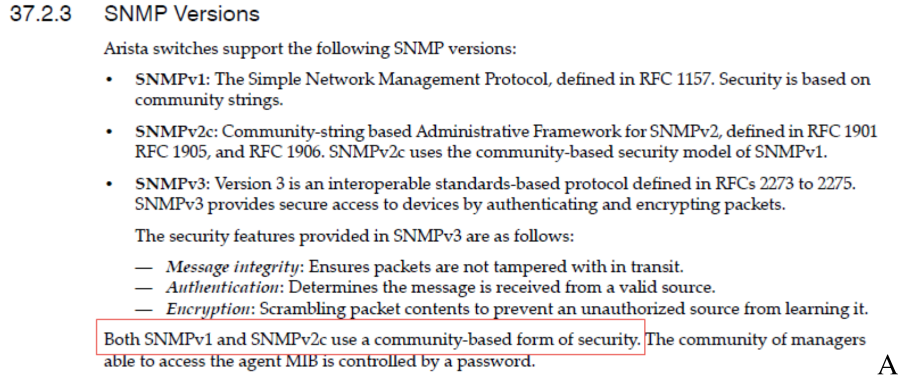
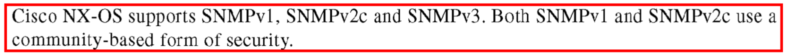
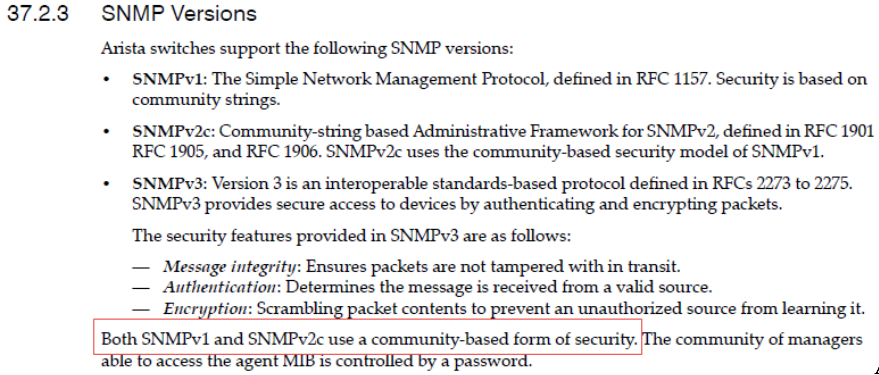
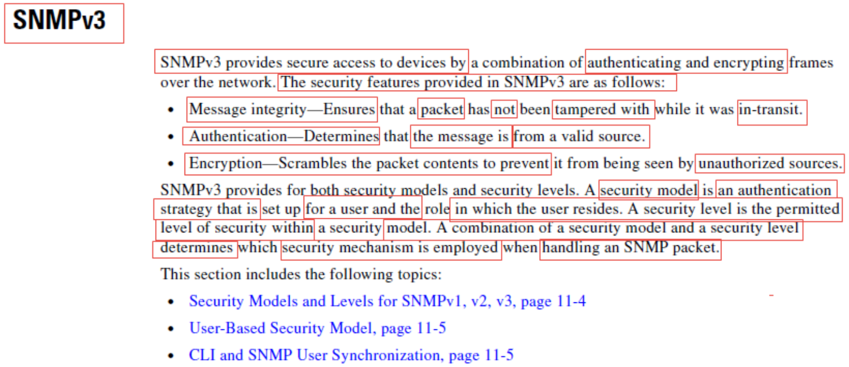
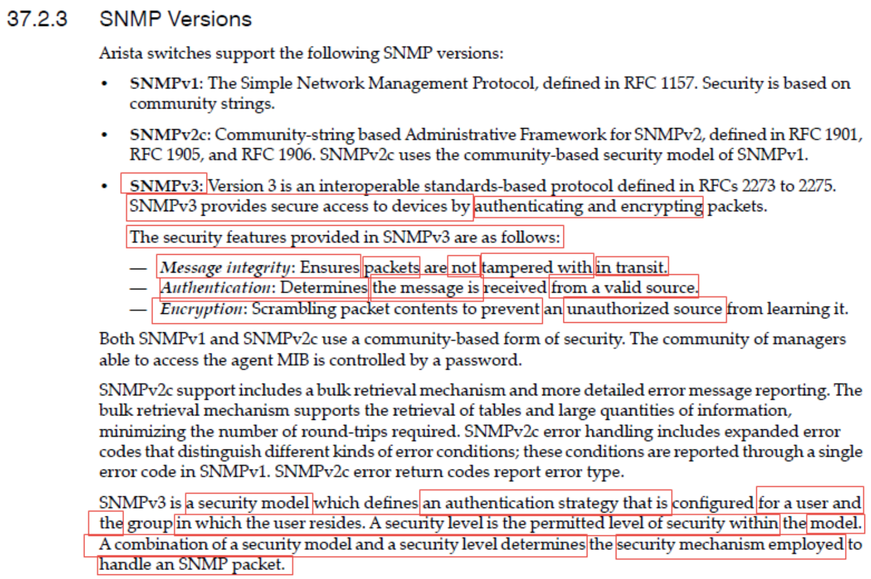
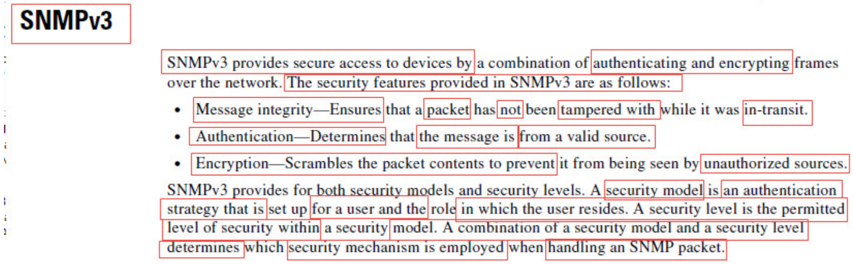
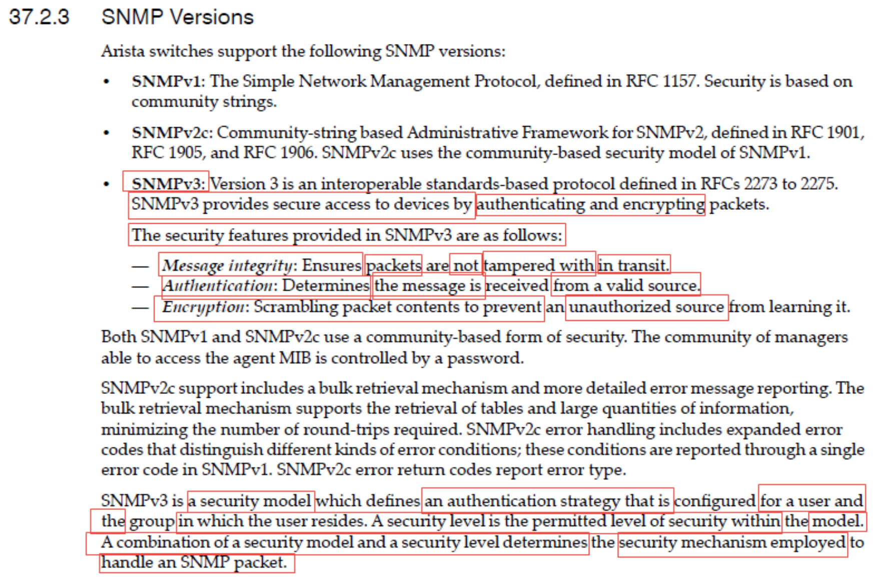
EXHIBITS A1-A6

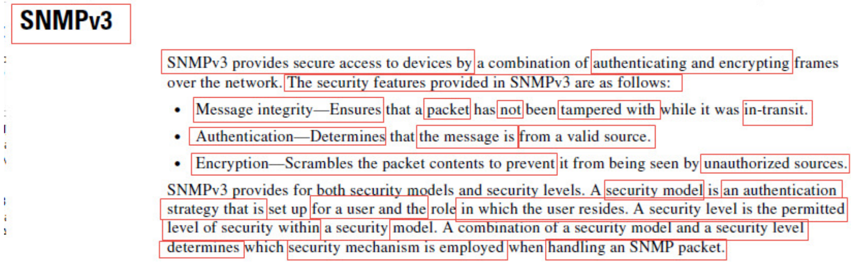
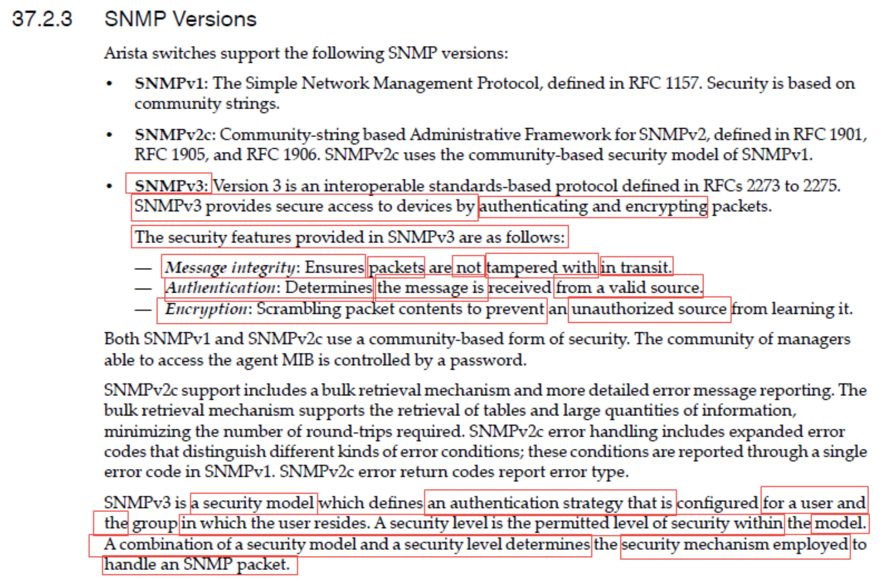
(Part 13 of 13)

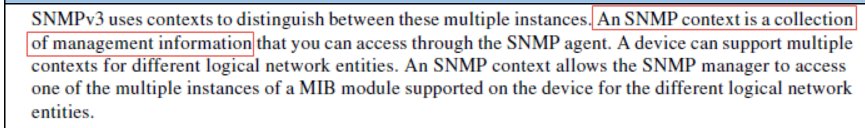
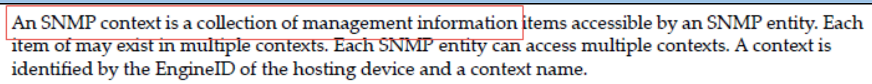
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **SNMP Functional Overview** The SNMP framework consists of three parts: • An SNMP manager—The system used to control and monitor the activities of network devices using SNMP. • An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. Cisco NX-OS supports the agent and MIB. To enable the SNMP agent, you must define the relationship between the manager and the agent. • A managed information base (MIB)—The collection of managed objects on the SNMP agent. SNMP is defined in RFCs 3411 to 3418. Cisco NX-OS supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. Cisco NX-OS supports SNMP over IPv6. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x (2010), at 10-2.	 37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1**: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c**: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901 RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3**: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891*;*Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.	Dkt. 419-10 at PDF p. 425

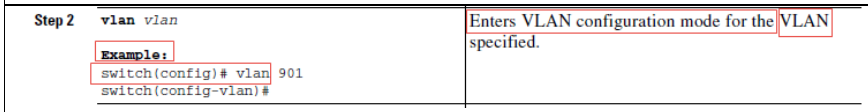
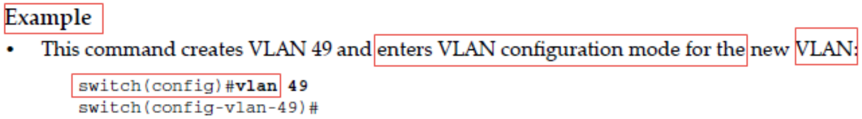
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 Cisco NX-OS supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0 (2008), at 10-2.	 37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1:** The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c:** Community-string based Administrative Framework for SNMPv2, defined in RFC 1901 RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3:** Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. A rista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891;Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.8.2 (11/18/11), at 675; Arista User Manual v. 4.7.3 (7/18/11), at 531.	Dkt. 419-10 at PDF p. 426

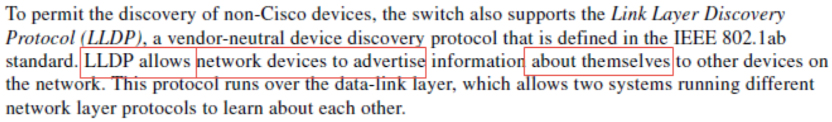
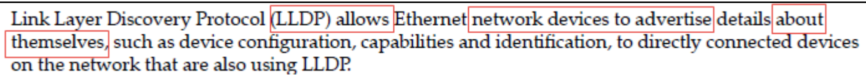
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **SNMPv3** SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows: • Message integrity—Ensures that a packet has not been tampered with while it was in-transit. • Authentication—Determines that the message is from a valid source. • Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources. SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. This section includes the following topics: • Security Models and Levels for SNMPv1, v2, v3, page 11-4 • User-Based Security Model, page 11-5 • CLI and SNMP User Synchronization, page 11-5 Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 11-3.	 37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1**: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c**: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3**: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. SNMPv2c error handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. SNMPv2c error return codes report error type. SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891*;*Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107-08; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.7.3 (7/18/11), at 531.	Dkt. 419-10 at PDF p. 427

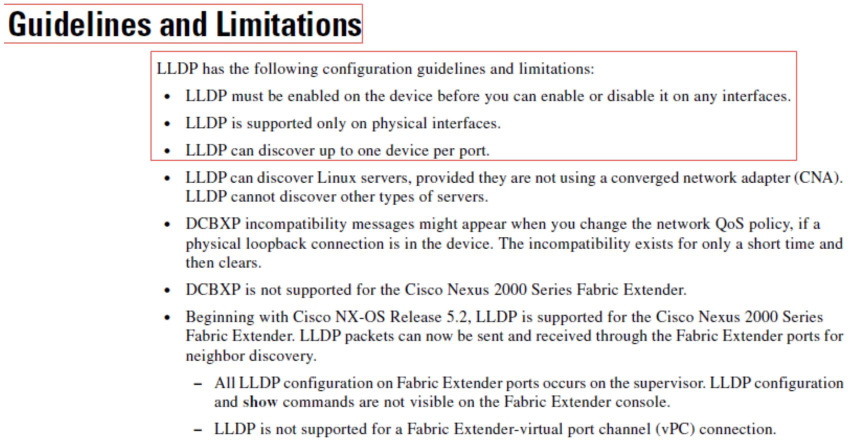
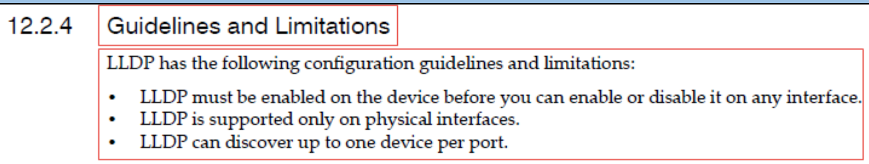
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **SNMPv3** SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows: • Message integrity—Ensures that a packet has not been tampered with while it was in-transit. • Authentication—Determines that the message is from a valid source. • Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources. SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x (2010), at 10-2.	 37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1:** The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c:** Community-string based Administrative Framework for SNMPv2, defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3:** Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. SNMPv2c error handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. SNMPv2c error return codes report error type. SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891*;*Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107-08; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.7.3 (7/18/11), at 531.	Dkt. 419-10 at PDF p. 428

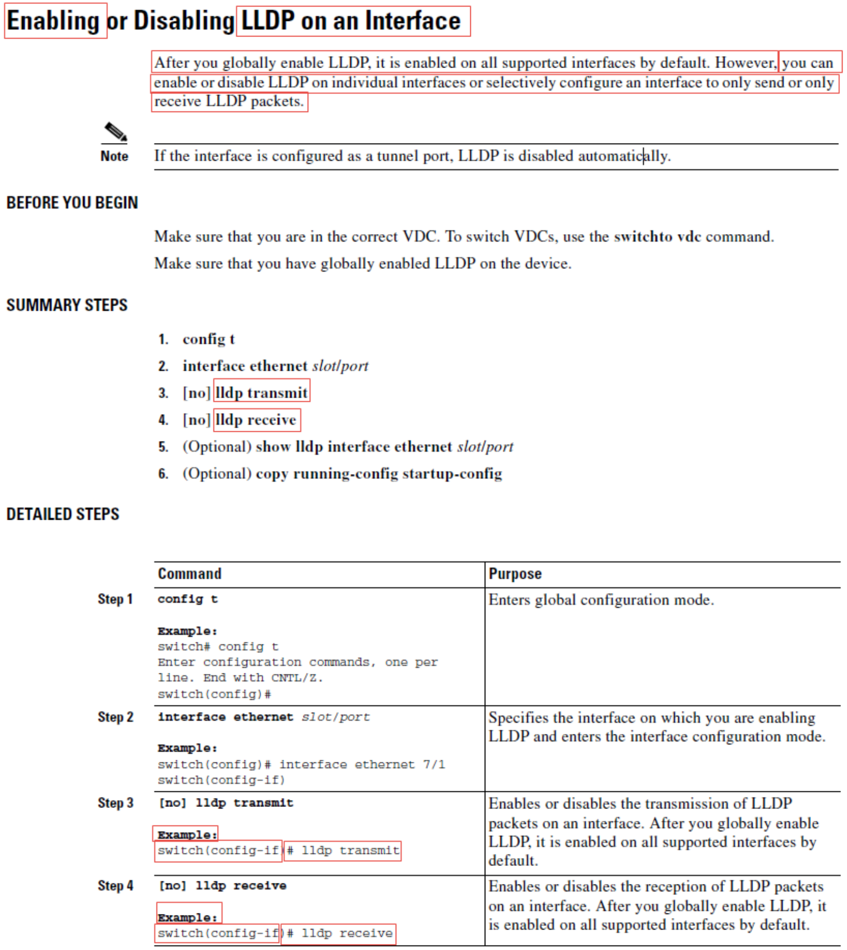
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **SNMPv3** SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows: • Message integrity—Ensures that a packet has not been tampered with while it was in-transit. • Authentication—Determines that the message is from a valid source. • Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources. SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0 (2008), at 7-2.	 37.2.3 SNMP Versions Arista switches support the following SNMP versions: • **SNMPv1**: The Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings. • **SNMPv2c**: Community-string based Administrative Framework for SNMPv2, defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c uses the community-based security model of SNMPv1. • **SNMPv3**: Version 3 is an interoperable standards-based protocol defined in RFCs 2273 to 2275. SNMPv3 provides secure access to devices by authenticating and encrypting packets. The security features provided in SNMPv3 are as follows: — *Message integrity*: Ensures packets are not tampered with in transit. — *Authentication*: Determines the message is received from a valid source. — *Encryption*: Scrambling packet contents to prevent an unauthorized source from learning it. Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent MIB is controlled by a password. SNMPv2c support includes a bulk retrieval mechanism and more detailed error message reporting. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required. SNMPv2c error handling includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. SNMPv2c error return codes report error type. SNMPv3 is a security model which defines an authentication strategy that is configured for a user and the group in which the user resides. A security level is the permitted level of security within the model. A combination of a security model and a security level determines the security mechanism employed to handle an SNMP packet. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 349. *See also* Arista User Manual v. 4.13.6F (4/14/2014), at 1891*;*Arista User Manual v. 4.12.3 (7/17/13), at 1654; Arista User Manual, v. 4.11.1 (1/11/13), at 1341; Arista User Manual v. 4.10.3 (10/22/12), at 1107-08; Arista User Manual v. 4.9.3.2 (5/3/12), at 863; Arista User Manual v. 4.7.3 (7/18/11), at 531.	Dkt. 419-10 at PDF p. 429

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 SNMPv3 uses contexts to distinguish between these multiple instances. An SNMP context is a collection of management information that you can access through the SNMP agent. A device can support multiple contexts for different logical network entities. An SNMP context allows the SNMP manager to access one of the multiple instances of a MIB module supported on the device for the different logical network entities. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 11-3.	 An SNMP context is a collection of management information items accessible by an SNMP entity. Each item of may exist in multiple contexts. Each SNMP entity can access multiple contexts. A context is identified by the EngineID of the hosting device and a context name. Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 1994. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 1684; Arista User Manual, v. 4.11.1 (1/11/13), at 1369; Arista User Manual v. 4.10.3 (10/22/12), at 1136; Arista User Manual v. 4.9.3.2 (5/3/12), at 892; Arista User Manual v. 4.8.2 (11/18/11), at 699; Arista User Manual v. 4.7.3 (7/18/11), at 555.	Dkt. 419-10 at PDF p. 429


Step 2 `vlan` *`vlan`* — Enters VLAN configuration mode for the VLAN specified.
Example:
`switch(config)# vlan 901`
`switch(config-vlan)#`
Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 16-18.
	
	Example
	• This command creates VLAN 49 and enters VLAN configuration mode for the new VLAN:
	`switch(config)#`**`vlan`**` 49`
	`switch(config-vlan-49)#`
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 803.
	See also Arista User Manual v. 4.12.3 (7/17/13), at 650; Arista User Manual, v. 4.11.1 (1/11/13), at 502; Arista User Manual v. 4.10.3 (10/22/12), at 420; Arista User Manual v. 4.9.3.2 (5/3/12), at 359.
		Dkt. 419-10 at PDF p. 430

 To permit the discovery of non-Cisco devices, the switch also supports the *Link Layer Discovery Protocol (LLDP)*, a vendor-neutral device discovery protocol that is defined in the IEEE 802.1ab standard. LLDP allows network devices to advertise information about themselves to other devices on the network. This protocol runs over the data-link layer, which allows two systems running different network layer protocols to learn about each other. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-2.	 Link Layer Discovery Protocol (LLDP) allows Ethernet network devices to advertise details about themselves, such as device configuration, capabilities and identification, to directly connected devices on the network that are also using LLDP. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 572. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 447; Arista User Manual, v. 4.11.1 (1/11/13), at 365.	Dkt. 419-10 at PDF p. 430

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 **Guidelines and Limitations** LLDP has the following configuration guidelines and limitations: • LLDP must be enabled on the device before you can enable or disable it on any interfaces. • LLDP is supported only on physical interfaces. • LLDP can discover up to one device per port. • LLDP can discover Linux servers, provided they are not using a converged network adapter (CNA). LLDP cannot discover other types of servers. • DCBXP incompatibility messages might appear when you change the network QoS policy, if a physical loopback connection is in the device. The incompatibility exists for only a short time and then clears. • DCBXP is not supported for the Cisco Nexus 2000 Series Fabric Extender. • Beginning with Cisco NX-OS Release 5.2, LLDP is supported for the Cisco Nexus 2000 Series Fabric Extender. LLDP packets can now be sent and received through the Fabric Extender ports for neighbor discovery. – All LLDP configuration on Fabric Extender ports occurs on the supervisor. LLDP configuration and **show** commands are not visible on the Fabric Extender console. – LLDP is not supported for a Fabric Extender-virtual port channel (vPC) connection. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-2.	 12.2.4 Guidelines and Limitations LLDP has the following configuration guidelines and limitations: • LLDP must be enabled on the device before you can enable or disable it on any interface. • LLDP is supported only on physical interfaces. • LLDP can discover up to one device per port. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 576. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 448; Arista User Manual, v. 4.11.1 (1/11/13), at 366.	Dkt. 419-10 at PDF p. 430

<table>
<tr><th>Cisco's Documentation</th><th>Arista's Documentation</th><th>Supporting Evidence In The Record</th></tr>
<tr>
<td>

<b>Enabling or Disabling LLDP on an Interface</b>

After you globally enable LLDP, it is enabled on all supported interfaces by default. However, you can enable or disable LLDP on individual interfaces or selectively configure an interface to only send or only receive LLDP packets.

Note: If the interface is configured as a tunnel port, LLDP is disabled automatically.

<b>BEFORE YOU BEGIN</b>

Make sure that you are in the correct VDC. To switch VDCs, use the <b>switchto vdc</b> command.
Make sure that you have globally enabled LLDP on the device.

<b>SUMMARY STEPS</b>

1. <b>config t</b>
2. <b>interface ethernet</b> <i>slot/port</i>
3. [<b>no</b>] <b>lldp transmit</b>
4. [<b>no</b>] <b>lldp receive</b>
5. (Optional) <b>show lldp interface ethernet</b> <i>slot/port</i>
6. (Optional) <b>copy running-config startup-config</b>

<b>DETAILED STEPS</b>

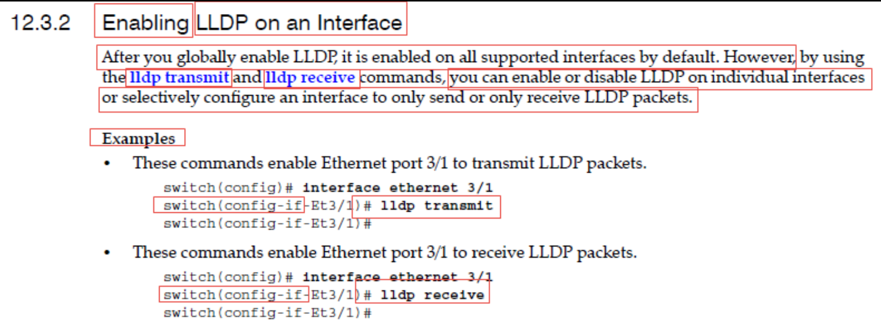
<table>
<tr><th></th><th>Command</th><th>Purpose</th></tr>
<tr><td>Step 1</td><td><b>config t</b>

<b>Example:</b>
switch# config t
Enter configuration commands, one per
line. End with CNTL/Z.
switch(config)#</td><td>Enters global configuration mode.</td></tr>
<tr><td>Step 2</td><td><b>interface ethernet</b> <i>slot/port</i>

<b>Example:</b>
switch(config)# interface ethernet 7/1
switch(config-if)</td><td>Specifies the interface on which you are enabling LLDP and enters the interface configuration mode.</td></tr>
<tr><td>Step 3</td><td><b>[no] lldp transmit</b>

<b>Example:</b>
switch(config-if)# lldp transmit</td><td>Enables or disables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.</td></tr>
<tr><td>Step 4</td><td><b>[no] lldp receive</b>

<b>Example:</b>
switch(config-if)# lldp receive</td><td>Enables or disables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.</td></tr>
</table>

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-6.
</td>
<td>

12.3.2 Enabling LLDP on an Interface

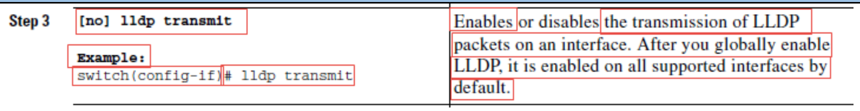
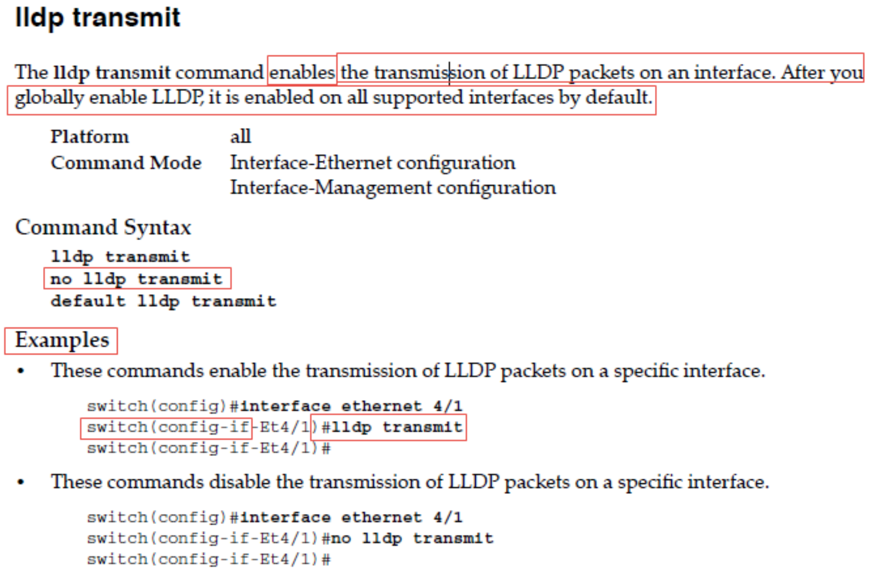
After you globally enable LLDP, it is enabled on all supported interfaces by default. However, by using the lldp transmit and lldp receive commands, you can enable or disable LLDP on individual interfaces or selectively configure an interface to only send or only receive LLDP packets.

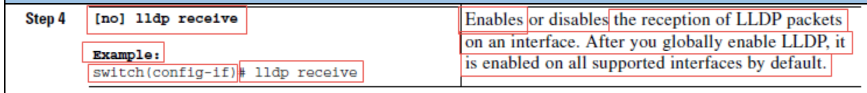
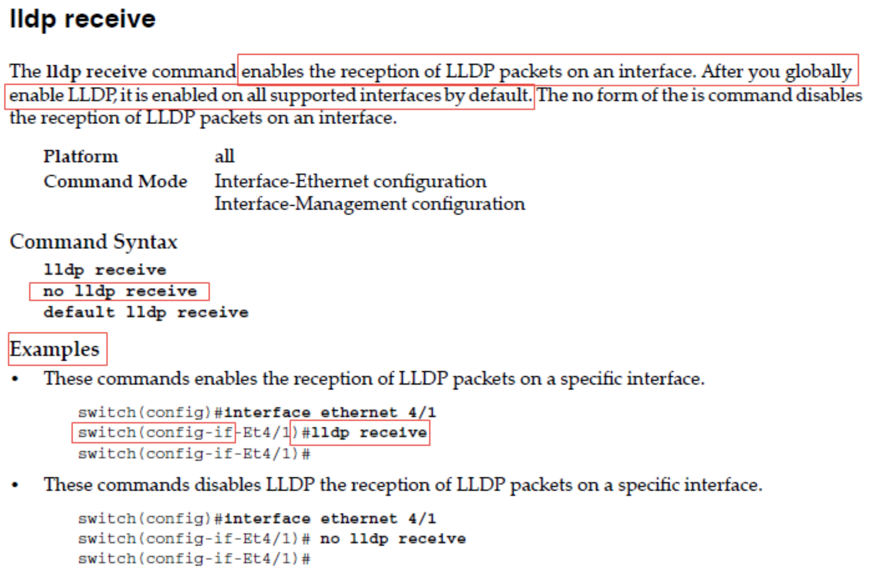
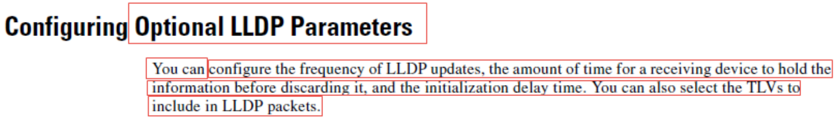
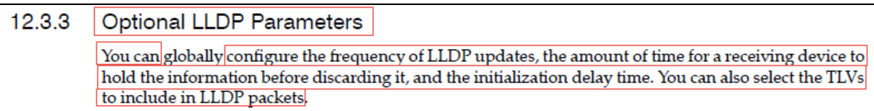
Examples
• These commands enable Ethernet port 3/1 to transmit LLDP packets.
switch(config)# <b>interface ethernet 3/1</b>
switch(config-if-Et3/1)# <b>lldp transmit</b>
switch(config-if-Et3/1)#
• These commands enable Ethernet port 3/1 to receive LLDP packets.
switch(config)# <b>interface ethernet 3/1</b>
switch(config-if-Et3/1)# <b>lldp receive</b>
switch(config-if-Et3/1)#

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 577.

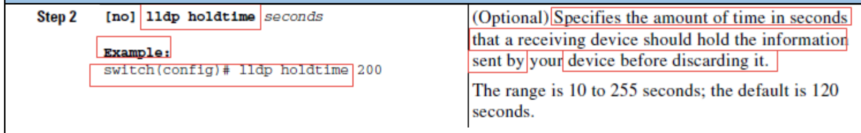
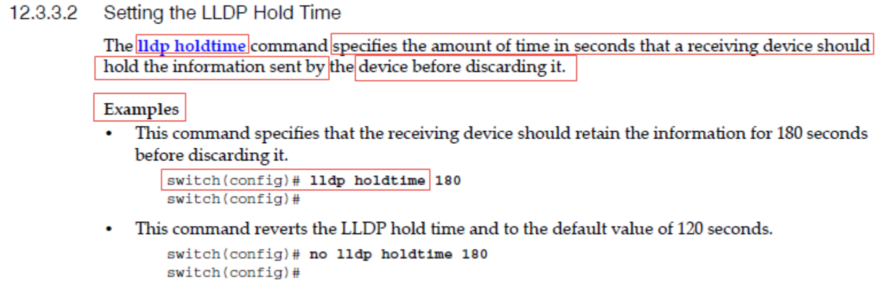
<i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 449; Arista User Manual, v. 4.11.1 (1/11/13), at 367.
</td>
<td>Dkt. 419-10 at PDF p. 431</td>
</tr>
</table>

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record

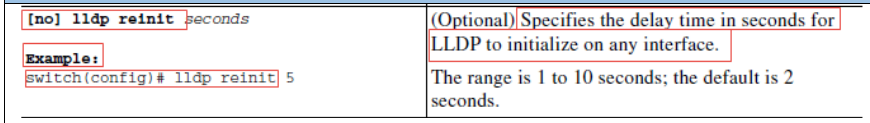
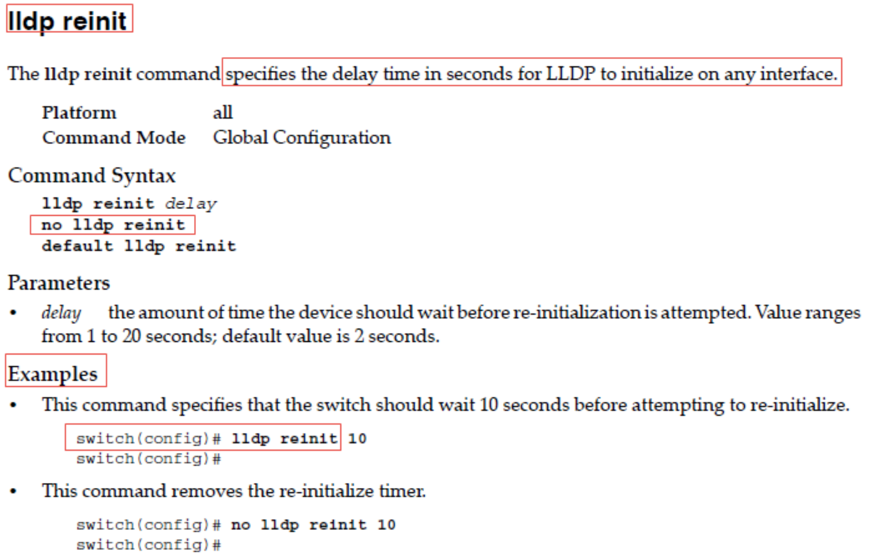

Step 3 `[no] lldp transmit`
Example:
`switch(config-if)# lldp transmit`
Enables or disables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.
Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-6.
	
	lldp transmit
	The **lldp transmit** command enables the transmission of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default.
	Platform all
	Command Mode Interface-Ethernet configuration
	Interface-Management configuration
	Command Syntax
	`lldp transmit`
	`no lldp transmit`
	`default lldp transmit`
	Examples
	• These commands enable the transmission of LLDP packets on a specific interface.
	`switch(config)#interface ethernet 4/1`
	`switch(config-if-Et4/1)#lldp transmit`
	`switch(config-if-Et4/1)#`
	• These commands disable the transmission of LLDP packets on a specific interface.
	`switch(config)#interface ethernet 4/1`
	`switch(config-if-Et4/1)#no lldp transmit`
	`switch(config-if-Et4/1)#`
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 593.
	See also Arista User Manual v. 4.12.3 (7/17/13), at 466; Arista User Manual, v. 4.11.1 (1/11/13), at 384.
		Dkt. 419-10 at PDF p. 432

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 Step 4 [no] lldp receive Example: switch(config-if)# lldp receive Enables or disables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-6.	 **lldp receive** The **lldp receive** command enables the reception of LLDP packets on an interface. After you globally enable LLDP, it is enabled on all supported interfaces by default. The no form of the is command disables the reception of LLDP packets on an interface. Platform all Command Mode Interface-Ethernet configuration Interface-Management configuration Command Syntax lldp receive no lldp receive default lldp receive Examples - These commands enables the reception of LLDP packets on a specific interface. switch(config)#interface ethernet 4/1 switch(config-if-Et4/1)#lldp receive switch(config-if-Et4/1)# - These commands disables LLDP the reception of LLDP packets on a specific interface. switch(config)#interface ethernet 4/1 switch(config-if-Et4/1)# no lldp receive switch(config-if-Et4/1)# Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 588. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 461; Arista User Manual, v. 4.11.1 (1/11/13), at 379.	Dkt. 419-10 at PDF p. 433
 **Configuring Optional LLDP Parameters** You can configure the frequency of LLDP updates, the amount of time for a receiving device to hold the information before discarding it, and the initialization delay time. You can also select the TLVs to include in LLDP packets. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-7.	 12.3.3 Optional LLDP Parameters You can globally configure the frequency of LLDP updates, the amount of time for a receiving device to hold the information before discarding it, and the initialization delay time. You can also select the TLVs to include in LLDP packets. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 577. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 449; Arista User Manual, v. 4.11.1 (1/11/13), at 367.	Dkt. 419-10 at PDF p. 433

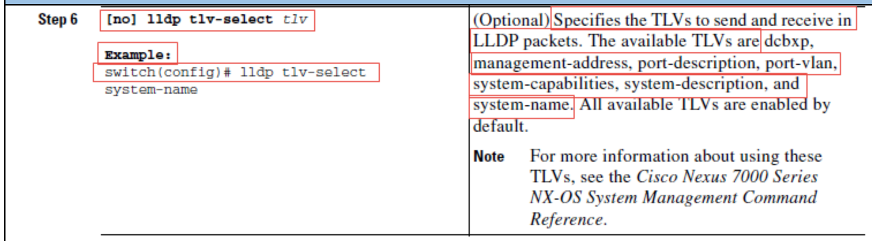
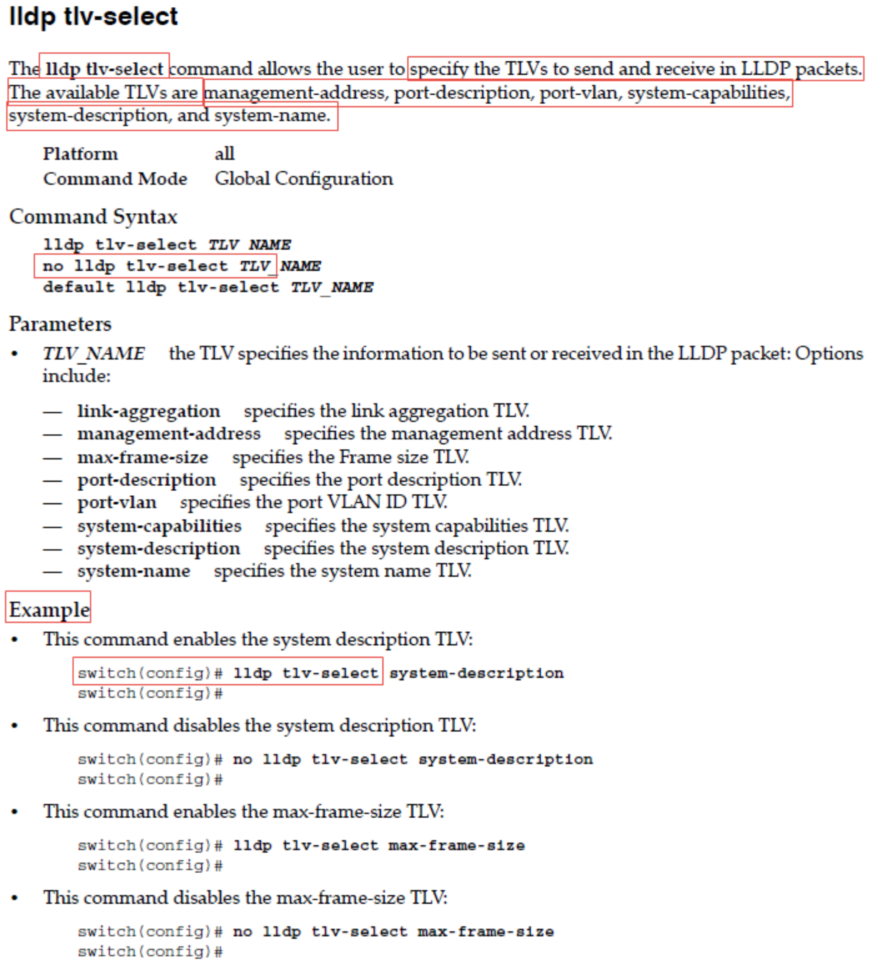
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record

 Step 2 **[no] lldp holdtime** *seconds*
Example:
`switch(config)# lldp holdtime 200`
(Optional) Specifies the amount of time in seconds that a receiving device should hold the information sent by your device before discarding it.
The range is 10 to 255 seconds; the default is 120 seconds.
Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-8.
	 12.3.3.2 Setting the LLDP Hold Time
	The lldp holdtime command specifies the amount of time in seconds that a receiving device should hold the information sent by the device before discarding it.
	Examples
	• This command specifies that the receiving device should retain the information for 180 seconds before discarding it.
	`switch(config)# lldp holdtime 180`
	`switch(config)#`
	• This command reverts the LLDP hold time and to the default value of 120 seconds.
	`switch(config)# no lldp holdtime 180`
	`switch(config)#`
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 578.
	See also Arista User Manual v. 4.12.3 (7/17/13), at 450; Arista User Manual, v. 4.11.1 (1/11/13), at 368.
		Dkt. 419-10 at PDF p. 434

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record


`[no] lldp reinit` *seconds* — (Optional) Specifies the delay time in seconds for LLDP to initialize on any interface.
The range is 1 to 10 seconds; the default is 2 seconds.
Example:
`switch(config)# lldp reinit 5`
 	
Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-8.
	
	lldp reinit
	The **lldp reinit** command specifies the delay time in seconds for LLDP to initialize on any interface.
	Platform all
	Command Mode Global Configuration
	Command Syntax
	`lldp reinit` *delay*
	`no lldp reinit`
	`default lldp reinit`
	Parameters
	• *delay* the amount of time the device should wait before re-initialization is attempted. Value ranges from 1 to 20 seconds; default value is 2 seconds.
	Examples
	• This command specifies that the switch should wait 10 seconds before attempting to re-initialize.
	`switch(config)# lldp reinit 10`
	`switch(config)#`
	• This command removes the re-initialize timer.
	`switch(config)# no lldp reinit 10`
	`switch(config)#`
	
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 589.
	
	See also Arista User Manual v. 4.13.6F (4/14/2014), at 318; Arista User Manual v. 4.12.3 (7/17/13), at 262; Arista User Manual, v. 4.11.1 (1/11/13), at 208.
		Dkt. 419-10 at PDF p. 434

Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record


Step 6 `[no] lldp tlv-select tlv`
Example:
`switch(config)# lldp tlv-select system-name`
(Optional) Specifies the TLVs to send and receive in LLDP packets. The available TLVs are dcbxp, management-address, port-description, port-vlan, system-capabilities, system-description, and system-name. All available TLVs are enabled by default.
Note For more information about using these TLVs, see the *Cisco Nexus 7000 Series NX-OS System Management Command Reference*.
Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-8.
	
	lldp tlv-select
	The **lldp tlv-select** command allows the user to specify the TLVs to send and receive in LLDP packets. The available TLVs are management-address, port-description, port-vlan, system-capabilities, system-description, and system-name.
	Platform all
	Command Mode Global Configuration
	Command Syntax
	`lldp tlv-select TLV_NAME`
	`no lldp tlv-select TLV_NAME`
	`default lldp tlv-select TLV_NAME`
	Parameters
	• *TLV_NAME* the TLV specifies the information to be sent or received in the LLDP packet: Options include:
	— **link-aggregation** specifies the link aggregation TLV.
	— **management-address** specifies the management address TLV.
	— **max-frame-size** specifies the Frame size TLV.
	— **port-description** specifies the port description TLV.
	— **port-vlan** specifies the port VLAN ID TLV.
	— **system-capabilities** specifies the system capabilities TLV.
	— **system-description** specifies the system description TLV.
	— **system-name** specifies the system name TLV.
	Example
	• This command enables the system description TLV:
	`switch(config)# lldp tlv-select system-description`
	`switch(config)#`
	• This command disables the system description TLV:
	`switch(config)# no lldp tlv-select system-description`
	`switch(config)#`
	• This command enables the max-frame-size TLV:
	`switch(config)# lldp tlv-select max-frame-size`
	`switch(config)#`
	• This command disables the max-frame-size TLV:
	`switch(config)# no lldp tlv-select max-frame-size`
	`switch(config)#`
	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 592.
	See also Arista User Manual v. 4.12.3 (7/17/13), at 465; Arista User Manual, v. 4.11.1 (1/11/13), at 383.
		Dkt. 419-10 at PDF p. 435

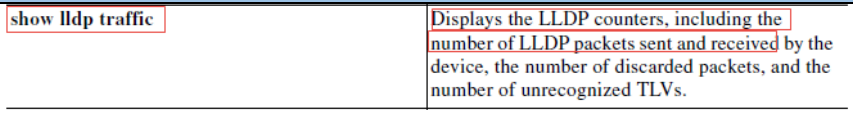
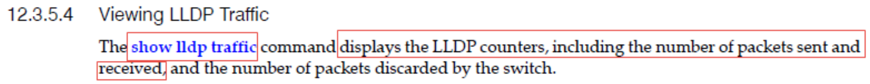
Cisco's Documentation	Arista's Documentation	Supporting Evidence In The Record
 show lldp traffic Displays the LLDP counters, including the number of LLDP packets sent and received by the device, the number of discarded packets, and the number of unrecognized TLVs. Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x (2013), at 18-9.	 12.3.5.4 Viewing LLDP Traffic The show lldp traffic command displays the LLDP counters, including the number of packets sent and received, and the number of packets discarded by the switch. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 581. *See also* Arista User Manual v. 4.12.3 (7/17/13), at 454; Arista User Manual, v. 4.11.1 (1/11/13), at 372.	Dkt. 419-10 at PDF p. 436

EXHIBIT A5

ARISTA'S VERBATIM COPYING OF CISCO'S COMMAND MODES & PROMPTS

Cisco Product	Cisco's Command Modes & Prompts	Arista's Command Modes & Prompts	Supporting Evidence In The Record
Router	**User EXEC >**	**EXEC >**	Dkt. 332-2 at PDF p. 52
Router	**Privileged EXEC #**	**Privileged EXEC #**	Dkt. 332-2 at PDF p. 52
Router	**Global Configuration (config)#**	**Global Configuration (config)#**	Dkt. 332-2 at PDF p. 52
Router	**Interface Configuration (config-if)#**	**Interface Configuration (config-if)#**	Dkt. 332-2 at PDF p. 52
Switch	**User EXEC >**	**EXEC >**	Dkt. 332-2 at PDF p. 52
Switch	**Privileged EXEC #**	**Privileged EXEC #**	Dkt. 332-2 at PDF p. 52
Switch	**EXEC #**	**Privileged EXEC #**	Dkt. 332-2 at PDF p. 52
Switch	**Global Configuration (config)#**	**Global Configuration (config)#**	Dkt. 332-2 at PDF p. 52
Switch	**Interface Configuration (config-if)#**	**Interface Configuration (config-if)#**	Dkt. 332-2 at PDF p. 52

EXHIBIT A6

ARISTA'S VERBATIM COPYING OF CISCO'S COMMAND HIERARCHIES[2]

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
aaa aaa accounting aaa accounting dot1x aaa authentication aaa authentication login aaa authorization config- commands aaa authorization console aaa group aaa group server radius aaa group server tacacs+	aaa aaa accounting aaa accounting dot1x aaa authentication aaa authentication login aaa authorization config- commands aaa authorization console aaa group aaa group server radius aaa group server tacacs+	Dkt. 332-2 at PDF pp. 257-259.

[2] Cisco has illustrated the command hierarchies in this table in this particular way in order to illustrate to the Court the relationship between the commands and show how they are sequenced, structured, and organized into hierarchies.

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
bgp bgp client-to-client reflection bgp cluster-id bgp confederation bgp confederation identifier bgp confederation peers bgp listen limit bgp log-neighbor-changes bgp redistribute-internal	bgp bgp client-to-client reflection bgp cluster-id bgp confederation bgp confederation identifier bgp confederation peers bgp listen limit bgp log-neighbor-changes bgp redistribute-internal (BGP)	Dkt. 332-2 at PDF pp. 260-261.

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
clear	clear	Dkt. 332-2 at PDF pp. 262-265.
clear arp-cache	clear arp-cache	
clear counters	clear counters	
clear ip	clear ip	
clear ip arp	clear ip arp	
clear ip bgp	clear ip bgp	
clear ip igmp group	clear ip igmp group	
clear ip mroute	clear ip mroute	
clear ip msdp sa-cache	clear ip msdp sa-cache	
clear ip nat translation	clear ip nat translation	
clear ip ospf neighbor	clear ip ospf neighbor	
clear ipv6	clear ipv6	
clear ipv6 neighbors	clear ipv6 neighbors	
clear ipv6 ospf force-spf	clear ipv6 ospf force-spf	
clear lldp	clear lldp	
clear lldp counters	clear lldp counters	
clear lldp table	clear lldp table	
clear mac-address-table dynamic	clear mac address-table dynamic	
clear spanning-tree counters	clear spanning-tree counters	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
dot1x dot1x max-reauth-req dot1x pae authenticator dot1x port-control dot1x reauthentication dot1x system-auth-control dot1x timeout dot1x timeout quiet-period dot1x timeout reauth-period dot1x timeout tx-period	dot1x dot1x max-reauth-req dot1x pae authenticator dot1x port-control dot1x reauthentication dot1x system-auth-control dot1x timeout dot1x timeout quiet-period dot1x timeout reauth-period dot1x timeout tx-period	Dkt. 332-2 at PDF pp. 266-267.
ip ip access ip access-group ip access-list ip access-list standard ip address ip as-path access-list ip community-list ip community-list expanded ip community-list standard ip dhcp smart-relay	ip ip access ip access-group ip access-list ip access-list standard ip address ip as-path access-list ip community-list ip community-list expanded ip community-list standard ip dhcp smart-relay	Dkt. 332-2 at PDF pp. 268-290.

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
ip dhcp smart-relay global	ip dhcp smart-relay global	
ip dhcp snooping	ip dhcp snooping	
ip dhcp snooping information option	ip dhcp snooping information option	
ip dhcp snooping vlan	ip dhcp snooping vlan	
ip domain	ip domain	
ip domain lookup	ip domain lookup	
ip domain name	ip domain name	
ip extcommunity-list	ip extcommunity-list	
ip extcommunity-list expanded	ip extcommunity-list expanded	
ip extcommunity-list standard	ip extcommunity-list standard	
ip helper-address	ip helper-address	
ip host	ip host	
ip http client source-interface	ip http client source-interface	
ip icmp redirect	ip icmp redirect	
ip igmp last-member-query	ip igmp last-member-query	
ip igmp last-member-query-count	ip igmp last-member-query-count	
ip igmp last-member-query-interval	ip igmp last-member-query-interval	
ip igmp query	ip igmp query	
ip igmp query-interval	ip igmp query-interval	
ip igmp query-max-response-time	ip igmp query-max-response-time	
ip igmp	ip igmp	
ip igmp snooping	ip igmp snooping	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
ip igmp snooping querier	ip igmp snooping querier	
ip igmp snooping vlan	ip igmp snooping vlan	
ip igmp snooping vlan immediate-leave	ip igmp snooping vlan immediate-leave	
ip igmp snooping vlan mrouter	ip igmp snooping vlan mrouter	
ip igmp snooping vlan static	ip igmp snooping vlan static	
ip igmp startup-query	ip igmp startup-query	
ip igmp startup-query-interval	ip igmp startup-query-interval	
ip igmp startup-query-count	ip igmp startup-query-count	
ip igmp static-group	ip igmp static-group	
ip igmp version	ip igmp version	
ip load-sharing	ip load-sharing	
ip local-proxy-arp	ip local-proxy-arp	
ip msdp	ip msdp	
ip msdp cache-sa-state	ip msdp cache-sa-state	
ip msdp default-peer	ip msdp default-peer	
ip msdp description	ip msdp description	
ip msdp group-limit	ip msdp group-limit	
ip msdp keepalive	ip msdp keepalive	
ip msdp mesh-group	ip msdp mesh-group	
ip msdp originator-id	ip msdp originator-id	
ip msdp peer	ip msdp peer	
ip msdp sa-filter	ip msdp sa-filter	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
ip msdp sa-filter in	ip msdp sa-filter in	
ip msdp sa-filter out	ip msdp sa-filter out	
ip msdp sa-limit	ip msdp sa-limit	
ip msdp shutdown	ip msdp shutdown	
ip msdp timer	ip msdp timer	
ip multicast	ip multicast	
ip multicast boundary	ip multicast boundary	
ip multicast-routing	ip multicast-routing	
ip name-server	ip name-server	
ip nat	ip nat	
ip nat pool	ip nat pool	
ip nat translation	ip nat translation	
ip nat translation tcp-timeout	ip nat translation tcp-timeout	
ip nat translation udp-timeout	ip nat translation udp-timeout	
ip ospf authentication	ip ospf authentication	
ip ospf authentication-key	ip ospf authentication-key	
ip ospf	ip ospf	
ip ospf bfd	ip ospf bfd	
ip ospf cost	ip ospf cost	
ip ospf dead-interval	ip ospf dead-interval	
ip ospf hello-interval	ip ospf hello-interval	
ip ospf message-digest-key	ip ospf message-digest-key	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
ip ospf name-lookup	ip ospf name-lookup	
ip ospf network	ip ospf network	
ip ospf priority	ip ospf priority	
ip ospf retransmit-interval	ip ospf retransmit-interval	
ip ospf shutdown	ip ospf shutdown	
ip ospf transmit-delay	ip ospf transmit-delay	
ip pim	ip pim	
ip pim anycast-rp	ip pim anycast-rp	
ip pim bfd	ip pim bfd	
ip pim bfd	ip pim bfd	
ip pim bfd-instance	ip pim bfd-instance	
ip pim bsr	ip pim bsr	
ip pim bsr-border	ip pim bsr-border	
ip pim bsr-candidate	ip pim bsr-candidate	
ip pim dr-priority	ip pim dr-priority	
ip pim log-neighbor-changes	ip pim log-neighbor-changes	
ip pim neighbor-filter	ip pim neighbor-filter	
ip pim query-interval	ip pim query-interval	
ip pim register-source	ip pim register-source	
ip pim rp	ip pim rp	
ip pim rp-address	ip pim rp-address	
ip pim rp-candidate	ip pim rp-candidate	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
ip pim sparse-mode	ip pim sparse-mode	
ip pim spt-threshold	ip pim spt-threshold	
ip pim spt-threshold group-list	ip pim spt-threshold group-list	
ip pim ssm range	ip pim ssm range	
ip prefix-list	ip prefix-list	
ip protocol	ip protocol	
ip proxy-arp	ip proxy-arp	
ip radius source-interface	ip radius source-interface	
ip rip v2-broadcast	ip rip v2-broadcast	
ip route	ip route	
ip routing	ip routing	
ip tacacs source-interface	ip tacacs source-interface	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
ipv6	ipv6	Dkt. 332-2 at PDF pp. 290-298.
ipv6 access-list[3]	ipv6 access-list	
ipv6 address	ipv6 address	
ipv6 dhcp relay destination	ipv6 dhcp relay destination	
ipv6 enable	ipv6 enable	
ipv6 host	ipv6 host	
ipv6 ipv6 access-group	ipv6 ipv6 access-group	
ipv6 nd	ipv6 nd	
ipv6 nd managed-config-flag	ipv6 nd managed-config-flag	
ipv6 nd ns-interval	ipv6 nd ns-interval	
ipv6 nd other-config-flag	ipv6 nd other-config-flag	
ipv6 nd prefix	ipv6 nd prefix	
ipv6 nd ra	ipv6 nd ra	
ipv6 nd ra interval	ipv6 nd ra interval	
ipv6 nd ra lifetime	ipv6 nd ra lifetime	
ipv6 nd ra suppress	ipv6 nd ra suppress	
ipv6 nd reachable-time	ipv6 nd reachable-time	
ipv6 nd router-preference	ipv6 nd router-preference	
ipv6 neighbor	ipv6 neighbor	
ipv6 ospf	ipv6 ospf	

[3] In Exhibit Copying 5 to the Opening Almeroth Report (Dkt. 332-2), this command expression was mislabeled under the "ip" hierarchy when it should have been included with the "ipv6" hierarchy, as shown here.

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
ipv6 ospf area ipv6 ospf cost ipv6 ospf dead-interval ipv6 ospf hello-interval ipv6 ospf network ipv6 ospf priority ipv6 ospf retransmit-interval ipv6 ospf transmit-delay ipv6 prefix-list ipv6 route ipv6 router ospf ipv6 unicast-routing	ipv6 ospf area ipv6 ospf cost ipv6 ospf dead-interval ipv6 ospf hello-interval ipv6 ospf network ipv6 ospf priority ipv6 ospf retransmit-interval ipv6 ospf transmit-delay ipv6 prefix-list ipv6 route ipv6 router ospf ipv6 unicast-routing	
neighbor neighbor activate neighbor allowas-in neighbor default-originate neighbor description neighbor ebgp-multihop neighbor fall-over bfd neighbor local-as neighbor next-hop-self	neighbor neighbor activate neighbor allowas-in neighbor default-originate neighbor description neighbor ebgp-multihop neighbor fall-over bfd neighbor local-as neighbor next-hop-self	Dkt. 332-2 at PDF pp. 299-304.

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
neighbor password neighbor peer-group neighbor peer-group (assigning members) neighbor peer-group (creating) neighbor remote-as neighbor remove-private-as neighbor route neighbor route-map neighbor route-reflector- client neighbor send-community neighbor shutdown neighbor soft-reconfiguration neighbor timers neighbor transport connection-mode neighbor update-source neighbor weight	neighbor password neighbor peer-group neighbor peer-group (assigning members) neighbor peer-group (creating) neighbor remote-as neighbor remove-private-as neighbor route neighbor route-map (BGP) neighbor route-reflector- client neighbor send-community neighbor shutdown neighbor soft-reconfiguration neighbor timers neighbor transport connection-mode neighbor update-source neighbor weight	
show show aaa show aaa method-lists show aaa sessions show arp show bfd neighbors	show show aaa show aaa method-lists show aaa sessions show arp show bfd neighbors	Dkt. 332-2 at PDF pp. 305-344.

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
show clock	show clock	
show dot1q-tunnel	show dot1q-tunnel	
show dot1x	show dot1x	
show dot1x all summary	show dot1x all summary	
show dot1x statistics	show dot1x statistics	
show environment	show environment	
show environment all	show environment all	
show environment cooling	show environment cooling	
show environment	show environment	
show environment power	show environment power	
show environment temperature	show environment temperature	
show etherchannel	show etherchannel	
show hostname	show hostname	
show hosts	show hosts	
show interfaces	show interfaces	
show interfaces capabilities	show interfaces capabilities	
show interfaces description	show interfaces description	
show interfaces flowcontrol	show interfaces flowcontrol	
show interfaces private-vlan mapping	show interfaces private-vlan mapping	
show interfaces status	show interfaces status	
show interfaces switchport	show interfaces switchport	
show interfaces switchport backup	show interfaces switchport backup	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
show interfaces transceiver	show interfaces transceiver	
show interfaces trunk	show interfaces trunk	
show inventory	show inventory	
show ip	show ip	
show ip access-lists	show ip access-lists	
show ip arp	show ip arp	
show ip bgp	show ip bgp	
show ip bgp community	show ip bgp community	
show ip bgp neighbors	show ip bgp neighbors (route type)	
show ip bgp neighbors	show ip bgp neighbors	
show ip bgp paths	show ip bgp paths	
show ip bgp peer-group	show ip bgp peer-group	
show ip bgp regexp	show ip bgp regexp	
show ip bgp summary	show ip bgp summary	
show ip community-list	show ip community-list	
show ip dhcp snooping	show ip dhcp snooping	
show ip extcommunity-list	show ip extcommunity-list	
show ip helper-address	show ip helper-address	
show ip igmp	show ip igmp	
show ip igmp groups	show ip igmp groups	
show ip igmp interface	show ip igmp interface	
show ip igmp snooping	show ip igmp snooping	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
show ip igmp snooping groups	show ip igmp snooping groups	
show ip igmp snooping mrouter	show ip igmp snooping mrouter	
show ip igmp snooping querier	show ip igmp snooping querier	
show ip interface	show ip interface	
show ip interface brief	show ip interface brief	
show ip mfib	show ip mfib	
show ip mroute	show ip mroute	
show ip mroute count	show ip mroute count	
show ip msdp	show ip msdp	
show ip msdp mesh-group	show ip msdp mesh-group	
show ip msdp peer	show ip msdp peer	
show ip msdp rpf-peer	show ip msdp rpf-peer	
show ip msdp sa-cache	show ip msdp sa-cache	
show ip msdp summary	show ip msdp summary	
show ip nat translations	show ip nat translations	
show ip ospf	show ip ospf	
show ip ospf border-routers	show ip ospf border-routers	
show ip ospf database database-summary	show ip ospf database database-summary	
show ip ospf interface	show ip ospf interface	
show ip ospf neighbor	show ip ospf neighbor	
show ip ospf request-list	show ip ospf request-list	
show ip ospf retransmission- list	show ip ospf retransmission- list	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
show ip pim	show ip pim	
show ip pim interface	show ip pim interface	
show ip pim neighbor	show ip pim neighbor	
show ip pim rp	show ip pim rp	
show ip pim rp-hash	show ip pim rp-hash	
show ip prefix-list	show ip prefix-list	
show ip rip	show ip rip	
show ip rip database	show ip rip database	
show ip rip neighbors	show ip rip neighbors	
show ip route	show ip route	
show ip route summary	show ip route summary	
show ip route tag	show ip route tag	
show ipv6	show ipv6	
show ipv6 access-list	show ipv6 access-list	
show ipv6 bgp	show ipv6 bgp	
show ipv6 bgp community	show ipv6 bgp community	
show ipv6 bgp neighbors	show ipv6 bgp neighbors	
show ipv6 bgp summary	show ipv6 bgp summary	
show ipv6 interface	show ipv6 interface	
show ipv6 neighbors	show ipv6 neighbors	
show ipv6 ospf	show ipv6 ospf	
show ipv6 ospf border- routers	show ipv6 ospf border- routers	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
show ipv6 ospf interface	show ipv6 ospf interface	
show ipv6 ospf neighbor	show ipv6 ospf neighbor	
show ipv6 prefix-list	show ipv6 prefix-list	
show ipv6 route	show ipv6 route	
show ipv6 route summary	show ipv6 route summary	
show ipv6 route tag	show ipv6 route tag	
show isis	show isis	
show isis database	show isis database	
show isis interface	show isis interface	
show isis topology	show isis topology	
show lacp	show lacp	
show lacp counters	show lacp counters	
show lacp interface	show lacp interface	
show lacp neighbor	show lacp neighbor	
show link state group	show link state group	
show lldp	show lldp	
show lldp neighbors	show lldp neighbors	
show lldp traffic	show lldp traffic	
show mac	show mac	
show mac access-list	show mac access-list	
show mac address-table	show mac address-table	
show mac address-table aging time	show mac address-table aging time	

Cisco’s Command Hierarchies	Arista’s Command Hierarchies	Supporting Evidence In The Record
show mac address-table count	show mac address-table count	
show module	show module	
show monitor session	show monitor session	
show ntp	show ntp	
show ntp associations	show ntp associations	
show ntp status	show ntp status	
show policy-map	show policy-map	
show policy-map control-plane	show policy-map control-plane	
show policy-map interface	show policy-map interface	
show policy-map interface control-plane	show policy-map interface control-plane	
show port	show port	
show port-channel	show port-channel	
show port-channel summary	show port-channel summary	
show port-channel traffic	show port-channel traffic	
show port-security	show port-security	
show port-security address	show port-security address	
show port-security interface	show port-security interface	
show privilege	show privilege	
show ptp	show ptp	
show ptp clock	show ptp clock	
show ptp parent	show ptp parent	
show ptp time-property	show ptp time-property	

Cisco’s Command Hierarchies	Arista’s Command Hierarchies	Supporting Evidence In The Record
show radius	show radius	
show redundancy states	show redundancy states	
show reload	show reload	
show role	show role	
show route-map	show route-map	
show snmp	show snmp	
show snmp chassis	show snmp chassis	
show snmp community	show snmp community	
show snmp contact	show snmp contact	
show snmp engineID	show snmp engineID	
show snmp group	show snmp group	
show snmp host	show snmp host	
show snmp location	show snmp location	
show snmp mib	show snmp mib	
show snmp source-interface	show snmp source-interface	
show snmp trap	show snmp trap	
show snmp user	show snmp user	
show snmp view	show snmp view	
show spanning-tree	show spanning-tree	
show spanning-tree blockedports	show spanning-tree blockedports	
show spanning-tree bridge	show spanning-tree bridge	
show spanning-tree interface	show spanning-tree interface	

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
show spanning-tree mst show spanning-tree mst configuration show spanning-tree mst interface show spanning-tree root show storm-control show tacacs show track show user-account show users show version show vlan show vlan private-vlan show vlan summary show vrf show vrrp	show spanning-tree mst show spanning-tree mst configuration show spanning-tree mst interface show spanning-tree root show storm-control show tacacs show track show user-account show users show version show vlan show vlan private-vlan show vlan summary show vrf show vrrp	
snmp-server snmp-server chassis-id snmp-server community snmp-server contact snmp-server enable traps snmp-server engineID snmp-server engineID local	snmp-server snmp-server chassis-id snmp-server community snmp-server contact snmp-server enable traps snmp-server engineID snmp-server engineID local	Dkt. 332-2 at PDF pp. 346-349.

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
snmp-server engineID remote snmp-server group snmp-server host snmp-server location snmp-server source-interface snmp-server user snmp-server view	snmp-server engineID remote snmp-server group snmp-server host snmp-server location snmp-server source-interface snmp-server user snmp-server view	
spanning-tree[4] spanning-tree bpdufilter spanning-tree bpduguard spanning-tree bridge assurance spanning-tree cost spanning-tree guard spanning-tree link-type spanning-tree loopguard default spanning-tree mode spanning-tree mst configuration	spanning-tree spanning-tree bpdufilter spanning-tree bpduguard spanning-tree bridge assurance spanning-tree cost spanning-tree guard spanning-tree link-type spanning-tree loopguard default spanning-tree mode spanning-tree mst configuration	Dkt. 332-2 at PDF pp. 349-353.

[4] In Exhibit Copying 5 to the Opening Almeroth Report (Dkt. 332-2), the following command expressions were mislabeled under the "snmp-server" hierarchy when they should have been included with the "spanning-tree hierarchies," as shown herein: spanning-tree bpdufilter, spanning-tree bpduguard, spanning-tree bridge assurance, spanning-tree cost, spanning-tree guard, spanning-tree link-type, spanning-tree loopguard default, spanning-tree mode, spanning-tree mst configuration, spanning-tree portfast bpdufilter default, spanning-tree portfast bpduguard default.

Cisco's Command Hierarchies	Arista's Command Hierarchies	Supporting Evidence In The Record
spanning-tree portfast spanning-tree portfast bpdufilter default spanning-tree portfast bpduguard default spanning-tree port-priority spanning-tree transmit hold- count spanning-tree vlan	spanning-tree portfast spanning-tree portfast bpdufilter default spanning-tree portfast bpduguard default spanning-tree port-priority spanning-tree transmit hold- count spanning-tree vlan	
vrrp vrrp authentication vrrp delay reload vrrp description vrrp ip vrrp ip secondary vrrp preempt vrrp priority vrrp shutdown vrrp timers advertise	vrrp vrrp authentication vrrp delay reload vrrp description vrrp ip vrrp ip secondary vrrp preempt vrrp priority vrrp shutdown vrrp timers advertise	Dkt. 332-2 at PDF pp. 354-356.